EXHIBIT A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 8,352,730	Examiner: To Be Assigned
Issued: January 8, 2013	Art Unit: To Be Assigned
Application No.: 11/314,199	
Filed: December 20, 2005	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**REQUEST FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 35 U.S.C. § 302 and 37 C.F.R. §§ 1.510 et seq., Samsung Electronics America, Inc. ("Samsung" or "Requestor") requests *ex parte* reexamination of claims 1-17 (the "Challenged Claims") of U.S. Patent No. 8,352,730 ("the '730 patent," Exhibit 1001), entitled "Biometric Personal Data Key (PDK) Authentication." The '730 patent issued on January 8, 2013, from Application No. 11/314,199, which was filed on December 20, 2005.

Patent Owner has asserted the '730 patent against Samsung and Samsung's parent, Samsung Electronics Co., Ltd., in *Proxense, LLC v. Samsung Electronics Co., Ltd., et. al*., Case No. 6:21-CV-00210-ADA (W.D. Tex.). Because the '730 patent is involved in concurrent litigation, the Patent Office should accord the requested reexamination "priority over all other cases." MPEP § 2261.

TABLE OF CONTENTS

Page

TABLE OF ATTACHMENTS AND EXHIBITS

Attachments

(1) Certificate of Service to Patent Owner
(2) Ex. 1011 Form PTO/SB/08a (Information Disclosure Statement)

Exhibits

The '730 patent, Declaration, and Prosecution History

Ex. 1001	U.S. Patent No. 8,352,730 ("'730 patent")
Ex. 1002	File History of the '730 patent
Ex. 1003	Expert Declaration of Dr. Benjamin Goldberg
Ex. 1004	CV of Dr. Benjamin Goldberg

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Other

Ex. 1009	Decision Denying Institution of *Inter Partes* Review, Paper 11, IPR 2021-01444 (Feb. 28, 2022)
Ex. 1010	Claim Construction Order in *Proxense, LLP v. Samsung Electronics Co., Ltd*, Case No. 6:21-CV-00210 (W.D. Tex.) Dkt. 43.
Ex. 1011	Form PTO/SB/08a (Information Disclosure Statement)
Ex. 1012	Introduction to Public Key Technology
Ex. 1013	Security Issues for Contactless Smart Cards
Ex. 1014	Smart Card Alliance Web Site
Ex. 1015	Smart Card Alliance Contactless Payment and the Retail Point of Sale

LISTING OF CLAIMS

CLAIM	LIMITATION
1a	A method for verifying a user during authentication of an integrated device, comprising the steps of:
1b	persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
1c	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
1d	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
1e	responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and
1f	responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a

CLAIM	LIMITATION
	casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
2	The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.
3	The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.
4	The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.
5	The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.
6	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.
7	The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric verification; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.

CLAIM	LIMITATION
8a	An integrated device for verifying a user during authentication of the integrated device, comprising:
8b	a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
8c	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and
8d	responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
9	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.

CLAIM	LIMITATION
10	The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.
11	The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.
12a	A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:
12b	receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;
12c	requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;
12d	receiving an access message from the agent; and
12e	in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino

CLAIM	LIMITATION
	machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
13	The method of claim 12, further comprising: registering a date of birth or age with the agent.
14	The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.
15a	A system, comprising:
15b	a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and
15c	if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or

CLAIM	LIMITATION
	more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and
15d	an authentication unit receives the plurality of codes and the other data values and send[] the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
15e	and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
16	The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.

CLAIM	LIMITATION
17	The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

I. INTRODUCTION

The challenged claims are directed to conventional technology to prevent unauthorized use of a wireless device by verifying both biometric information and the device itself. None of the concepts in the '730 patent were new when the patent was filed; they are clearly disclosed in prior art references that together disclose each and every element of the challenged claims. Moreover, all of the concepts in the patents were used for various different applications for years before the '730 patent was filed. Nevertheless, Patent Owner has launched a lawsuit against Samsung, alleging infringement of technology far newer and more innovative than the technology described in the challenged claims.

The lawsuit against Samsung involves five patents, all relating to similar technology. After the lawsuit against Samsung was filed, Samsung filed IPRs against all five asserted patents. Two of the IPRs were instituted (against US Patent Nos. 9,049,188 and 9,235,700) and are currently pending. The Board denied institution, however, on the '730 patent and two additional related family members: U.S. Patent Nos. 9,298,905 and 10,698,989. In the decisions not to institute the IPRs, the Board found merit in the Patent Owner's argument (which Samsung did not foresee, as it contradicted Patent Owner's claim construction arguments in litigation) that the prior art did not disclose a "third party trusted authority." The

present petition addresses Patent Owner's new argument with different prior art, and therefore presents substantial new questions of patentability.

This Request presents several substantial new questions of patentability. All four SNQs rely primarily on a new reference (Ludtke) that was cited neither during prosecution of either the '730 patent or any of its parents nor in the prior IPR petition regarding the '730 patent. Specifically, SNQ 1 relies on a combination of Ludtke and Okereke, neither of which was presented in the IPR. SNQ 2 relies on a third reference for a single limitation found in a handful of dependent claims. SNQs 3 and 4 rely on a combination of Ludtke and Scott, and while the Scott reference was presented in the IPR, it is cited here only as a secondary reference. Like SNQ 2, SNQ 4 relies on a third reference for a single limitation in a number of dependent claims. Respectfully, these combinations present substantial new questions of patentability that have not been considered by either the PTO or the PTAB.

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510

This request for *ex parte* reexamination of the '730 patent satisfies each requirement of 37 C.F.R. § 1.510.

A. Payment of Fees – 37 C.F.R. § 1.510(a)

Requestor authorizes the Patent and Trademark Office to charge Deposit Account No. DA505708 for the fees set in 37 C.P.R. § 1.20(c)(1) for reexamination.

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1)

A detailed discussion of pertinent new teachings in the prior art references that present substantial new questions of patentability is provided in Section X.

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2)

Samsung respectfully requests reexamination of claims 1-17 of the '730 patent based on the following proposed rejections:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. § 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. § 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. (a), (b), and (e) and 35 U.S.C. § 103.

A detailed explanation of the pertinence and manner of applying the cited prior art to claims 1-17 of the '730 patent is provided in Section X.

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3)

A copy of every patent or printed publication relied upon as a basis of unpatentability are submitted as exhibits in conjunction with this request for reexamination. In addition, a Form PTO/SB/08a is attached hereto as Exhibit 1011. A full list of exhibits appears on page 16.

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4)

A copy of the '730 patent is attached to this Request as Exhibit 1001.

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5)

The signature on this request certifies that a copy of the request has been served in its entirety on PO's representative at the address provided for in 37 C.F.R. § 1.33(c). Specifically, PO's representative was served by first-class U.S. mail on June 8, 2022, addressed to PO's attorney of record:

Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City, UT 84107

The Requester has also provided courtesy copies to PO's counsel in the aforementioned litigation by first-class U.S. mail on June 8, 2022, addressed to:

Hecht Partners
David Hecht
125 Park Avenue, 25th Floor
New York, NY 10017

Susman Godfrey
Brian Melton
1000 Louisiana St, Suite 5100
Houston, TX 77002

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6)

Samsung certifies that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) and 325(e)(1) do not prohibit it from filing this ex parte reexamination request.

Requestor previously filed one petition for *inter partes* review against the '730 patent. *See* IPR2021-01444. The petition was denied institution.

III. PROCEDURAL HISTORY

Requestor is unaware of any co-pending Patent Office proceedings involving the '730 patent. This is the first reexamination request challenging the claims of the '730 patent.

The '730 patent claims priority to two provisional patents: U.S. Patent Application Nos. 60/637,538, filed on Dec. 20, 2004, and 60/652,765, filed on Feb. 14, 2005. The application that led to the '730 patent was filed on December 20, 2005. The '730 patent issued on January 8, 2013.

A. Prosecution History of the '730 Patent

The application that led to the '730 Patent was filed on December 20, 2005. Ex. 1002 at 760-61.

On April 27, 2009, after lengthy exchanges regarding various formalities, the U.S. Patent & Trademark Office (hereinafter "Patent Office") issued the first non-final Office Action rejecting claims 1-21 under both 35 U.S.C. §§ 102 and 103 in light of Hsu et al. (U.S. Patent No. 6,041,410) in view of Saito et al. (US 20040129787). *See* Ex. 1002 at 475-93.

After a series of amendments and further rejections based on Stanko (US 2005/0074126) and Beenau et al. (US 2004/0230488), the Patent Office issued a Notice of Allowance on August 31, 2012. Ex. 1002 at 24-26, 88-103, and 258-72.

B. The IPR filed against the '730 Patent

Samsung previously filed an IPR against the '730 patent. IPR2021-01444. The IPR presented four grounds. The first three grounds were based on the Scott reference, combined with others. The fourth ground was based on the Berardi reference in combination with others. The PTAB denied institution of the first

three grounds based on its belief that none of the cited prior art disclosed a "third party trusted authority" with respect to claim 1. *See, e.g.*, IPR2021-01444, Paper 11 at 22-29. The PTAB denied institution on the fourth ground for unrelated reasons. *See, e.g.,* IPR2021-01444, Paper 11 at 30-33.

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES

Patent Owner may argue that this request should be denied in accordance with § 325(d) based on the Federal Circuit's decision in *In re Vivint, Inc.*, 14 F.4th 1342 (Fed. Cir. 2021). That case, however, does not apply here. In *Vivint,* the Requestor filed an *Ex Parte* Reexam request after filing a series of vexatious IPR petitions, the last of which the Board found was an "undesirable, incremental" attack on the Patent Owner. The Board reasoned that allowing such practices "risks harassment of patent owners and frustration of Congress's intent in enacting [the AIA]," and therefore denied the petition. *Id.* at 1346.

Notwithstanding that denial, the Requestor in *Vivint* filed a reexam request that ultimately resulted in cancellation of the challenged claims. On review, the Federal Circuit reversed the CRU's decision to grant the reexam, finding that the request, just like the denied IPR petition, was an abusive filing. The Federal Circuit noted that the vast majority of the reexam was a copy of the denied IPR petition, and the Court concluded that the Director's finding that the IPR petition

was abusive should have likewise applied to the reexam request. Specifically, the Court found that the reexam "copied, word-for-word, two grounds from the [denied IPR petition]--the very petition deemed 'a case of undesirable, incremental petitioning.'" *Id.* at 1353. And, for the portions that were not copied, the EPR "used prior Board decisions as a roadmap to correct past deficiencies." *Id.*

The facts here are distinguishable. ***First***, and most importantly, Samsung's previous IPR petition was not a series of "serial" petitions that were "undesirable, incremental petitions." There was only a single prior IPR filed on the '730 patent.

Second, this request is not a "word-for-word" copy of the denied IPR petition. To the contrary, the first SNQ in this request includes *completely new* art that was not seen in either prosecution or the prior IPR. In all four SNQs presented in this reexam, the primary reference, Ludtke, is completely new and was not considered during prosecution or presented in the previously filed IPR. Although the Scott reference was previously used in the prior IPR, it is used here only as a secondary reference in two SNQs. Similarly, the Robinson reference, which was used for a very specific limitation found in a handful of dependent claims, is also used for that same limitation in the dependent claims. Notably, the Board did not disagree that Robinson teaches that limitation.

Third, this reexam is not using the prior, denied '730 IPR petition as a "roadmap" to correct past deficiencies. In *Vivint*, the requestor copied, word-for-word, two grounds in their entirety, which the Board had already found to be vexatious harassment. Even in the portions that were not copied, the Board found that the same or similar prior art was used. Here, Samsung's request presents entirely new proposed SNQs of rejection. There are ***no*** SNQs that are "word-for-word" copies of the IPR grounds, and indeed, the primary reference that forms the vast basis for the rejections is entirely different and thus do not, and could not, use the prior IPR petition denial as a "roadmap."

Fourth**,** each of the above patents and publications are prior art to the Asserted Patents, and as mentioned above, the grounds of rejection outlined in this Request raise substantial new questions of patentability, because the reference combinations used to establish these grounds provide teachings not previously considered by the Office. None of the reference combinations used to establish the grounds for rejection in this Request, nor the grounds themselves, were advanced by the Examiner during prosecution of the applications that matured into the Asserted Patents.

Further, the references are also non-cumulative because, as discussed in more detail below, the prior art reference individually and/or in combination

disclose each and every limitation of the challenged claims—including the challenged independent claims that were allowed over the considered prior art.

For these reasons, the present request should not be denied pursuant to the CRU's discretionary powers.

V. LEVEL OF SKILL IN THE ART

The '730 patent claims priority to two provisional applications filed on December 20, 2004, and February 14, 2005. A person of ordinary skill in the art ("POSITA") at that time would have had a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). More education could compensate for less experience and vice versa. Ex. 1003 at ¶13 Each of the arguments below is made from the standpoint of a POSITA in the field of the '730 patent. Requestor's expert, Dr. Benjamin Goldberg, was at least a POSITA at the time of the alleged invention. *Id.*; Ex. 1004.

VI. CLAIM CONSTRUCTION

The USPTO construes claims in accordance with their "broadest reasonable interpretation" ("BRI") in light of the claim language and specification. *In re Reuter*, 670 F.2d 1015, 1019 (C.C.P.A. 1981); *In re Smith International, Inc.*, 871 F.3d 1375, 1381, 1382-83 (Fed. Cir. September 26, 2017). This is as true in reexamination proceedings as it is during original prosecution. *In re Am. Acad. of Sci. Tech Ctr.*,

367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1379 (Fed. Cir. 2007). The USPTO broadly interprets claims during examination of a patent application because the applicant may "amend his claims, the thought being to reduce the possibility that, after the patent is granted, the claims may be interpreted as giving broader coverage than is justified." *In re Prater*, 415 F.2d 1393, 1404-05 (C.C.P.A. 1969). According to the Federal Circuit, "[t]his approach serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified. Applicants' interests are not impaired since they are not foreclosed from obtaining appropriate coverage for their invention with express claim language." *In re Yamamoto*, 740 F.2d 1569, 1571-72 (Fed. Cir. 1984) (*citing In re Prater*, 415 F.2d at 1405 n.31). The same policy underpinning the use of the broadest-reasonable-interpretation standard in initial examination justifies its application in reexamination. *Id.*

Since the filing of the IPR, the District Court has issued a claim construction order construing terms as follows:[1]

Claims	**Term**	**Construction**
1,3,8,10,12,15	"device ID code"	A unique code identifying a device

[1] Other terms addressed by the Court were given their plain and ordinary meaning, or no construction was necessary.

1,8,12,15	"access message"	A signal or notification enabling or announcing access

Ex. 1010 at 3. In addition to these terms, the Court also construed a number of terms as having their "plain meaning." *Id*. Although the terms above have been construed according to the *Phillips* standard, Requestor has applied these constructions in the discussion below, as the Broadest Reasonable Interpretation encompasses the *Phillips* standard. Accordingly, if the prior art meets the limitations construed according to the *Phillips* standard, it meets the limitations construed according to BRI.

A. "third party trusted authority" (claims 1, 8, 12, and 15)

In the previous IPR, the PTAB construed the term "third party trusted authority" as "an entity or party separate from the principal parties to a transaction." Ex. 1009, IPR2021-01444, Paper 11 at 14. In considering the prior art in light of its construction of the term, the PTAB found that Petitioner did not "explain[] sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application is being permitted to access in the asserted combination." *Id*. at 26.[2] The Patent Owner argued that the DPC in

[2] Lapsley was the prior art reference that was relied upon for the "third party trusted authority" limitation in the IPR.

Lapsley (which Petitioner pointed to as the "third party trusted authority") actually acted as a "cloud based digital wallet," and further that the purchaser did not access the digital wallet using a "fob" or "phone," but rather a device in the store where they were purchasing something. Ex. 1009 at p. 26. Based on these arguments, the PTAB found that the "the DPC is the resource to be accessed" and that "it is a party to the transaction, rather than a third party." *Id*. The PTAB further observed that during prosecution, the applicant explained that a "user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *Id*. at 26-27; *see also* Ex. 1002 at. 434.

Requestor has applied this construction, in light of the Board's observations and analysis, to the prior art below.

VII. PRIORITY DATE OF THE '730 PATENT

The '730 patent claims priority to two provisional applications: U.S. Patent Application No. 60/637,538, filed December 20, 2004, and U.S. Patent Application No. 60/652,765, filed on February 14, 2005. Although Requestor does not concede that all 17 claims are entitled to one or both of the priority dates of the provisional applications, all prior art references relied on in this petition date back to before December 20, 2004, and therefore, no further determination needs to be made regarding the priority date.

VIII. OVERVIEW OF THE TECHNOLOGY

The '730 patent relates to integrated wireless devices in a generic "computerized authentication" system that is used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 at 1:15-18, 1:51-53. The integrated device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:59-64. After validation using the biometric scan, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* at 1:64-67. The device transmits the code to a third-party trusted authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 2:1-4. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* at 2:4-5. The '730 patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:28-30. The patent also purports to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:41-43.

IX. OVERVIEW OF THE PRIOR ART

A. Ludtke (Ex. 1005)

U.S. Patent No. 7,188,110 ("Ludtke") was filed on December 11, 2000. It issued on March 6, 2007. It is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

Titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," Ludtke discloses a method of identifying an authorized user with a biometric device and enabling the authorized user to access private information. Ex. 1005 at Abstract. Ludtke recognizes both the need to ensure the integrity of financial information and the privacy of the user. *Id*. at 1:11-20.

The system disclosed in Ludtke is strikingly like the system disclosed in the '730 Patent. The Ludtke system allows transactions through an eCommerce system through a "transaction device" that has a unique identifier (ID). *Id*. at 3:34-35. The transaction device can be a privacy card or a digital wallet or both. *Id*. at 35-39. This transaction device is a wireless device that is carried and maintained by a user. *See, e.g., id.* at 5:40-44. The transaction device includes a highly secured memory that can provide a transaction processing clearing house (TPCH) the necessary information to authorize a transaction. *Id.* at 3:40-45. The Ludtke system is described in Figure 1:

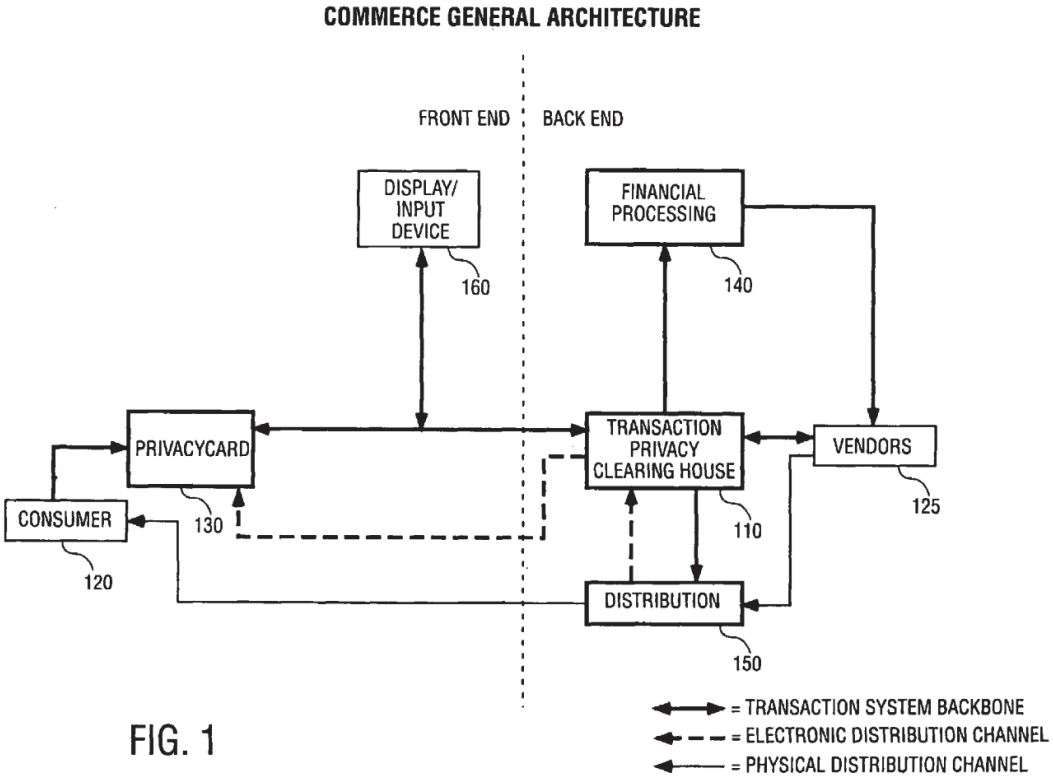


FIG. 1

As demonstrated in this figure, the Consumer 120 uses a transaction device 130 (in this figure, shown as a privacy card). The consumer wishes to purchase something from a vendor 125. The transaction device provides information to the TPCH for authorization for the transaction between the consumer and vendor to be performed. *Id*. at 6:36-44. The TPCH is not part of the transaction, but rather functions as a third-party middleman of the transaction. *Id*. at 7:44-46. This ensures that sensitive information is not shared with the vendor. *Id.* at 7:46-48.

Recognizing the need to protect the authorization of a user, Ludtke also discloses the use of fingerprint recognition as part of the digital wallet. *Id*. at 18:16-17. This biometric verification occurs before any transaction can take place, and therefore authorizes the user before the transaction device authorizes the device with the TPCH. *Id.* at 25:65-26:9.

B. Okereke (Ex. 1006)

U.S. Publication No. 2003/0196084 ("Okereke") was filed April 11, 2003. It published October 16, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA.

Okereke describes a "system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure[PKI]" and also indicates that it "facilitates secure remote communications." Ex. 1006 at Abstract. Okereke states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data." *Id*. at ¶3.

In setting up communications for a mobile device, Okereke specifically teaches that "a unique identifier for the wireless product to be employed is passed [sic] at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other

device capable of remote wireless communication. The unique identifier can be a serial number or SIM." *Id*. at ¶ 25.

Okereke describes the PKI: "With PKI, a public and private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted by the private key can only be decrypted with the corresponding public key. … The private key is given only to the requesting party and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network." *Id*. at ¶ 7. Therefore, the private key is secret information. Ex. 1003 at ¶45.

C. Robinson (Ex. 1007)

U.S. Publication No. 2003/0177102 ("Robinson") was filed February 19, 2003. It published September 18, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

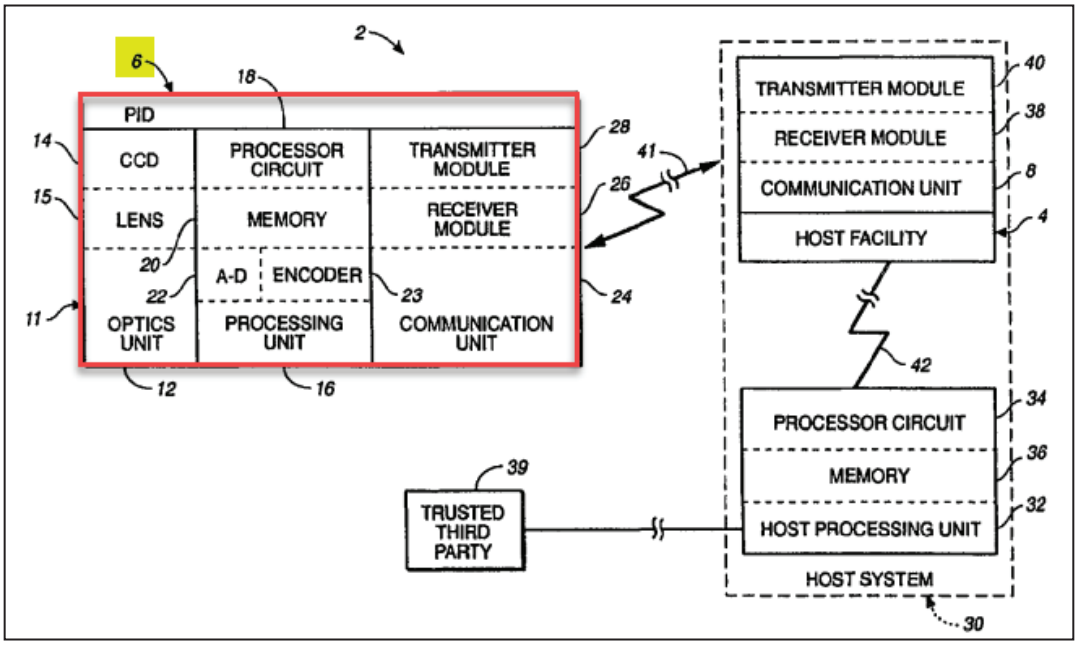
Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents

biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user.

D. Scott (Ex. 1008)

International PCT Application WO 99/56429 ("Scott") was filed on April 26, 1999. It was published on November 4, 1999. The International Publication Date is November 4, 1999, making it prior art under 35 U.S.C. § 102(b) (pre-AIA).

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.[3]

1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson

SNQ 1 involves combining the Ludtke and Okereke references, and SNQ 2 involves combining the Ludtke, Okereke, and Robinson references. Ludtke, Okereke, and Robinson all relate to protecting confidential information, communication over wireless networks, and the use of biometric information to protect this communication. All three references relate to communications for the purpose of financial transactions. Ex. 1005 at 4:54-56, 6:51-67; Ex. 1006 at ¶3; Ex. 1007 at ¶¶31-32, 47, Fig.1. A POSITA would naturally consider the teachings of Ludtke, Okereke, and Robinson in order to get a full understanding of the available options for secure communications and would have been motivated by this to combine the references' teachings. As explained in detail below, a POSITA would have considered applying the teachings of Okereke and Robinson to the teachings of Ludtke.

[3] Annotations are added to figures unless indicated otherwise.

2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson

SNQ 3 involves combining the Ludtke and Scott references, and SNQ 4 involves combining the Ludtke, Scott, and Robinson references. Ludtke, Scott, and Robinson also relate to protecting confidential information over wireless networks, using biometric information to protect sensitive information, and also relates to financial information. Ex. 1005 at 4:54-56, 6:51-67; Ex. 1007 at ¶¶31-32, 47, Fig.1; Ex. 1008 at 10:24-32, 18:29-19:20. Therefore, a POSITA would have combined the Scott reference with Ludtke and Robinson for the same reasons above with respect to Okereke. In fact, a POSITA would have considered all of these references in trying to develop a process of secure communications.

X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS

As shown in detail below, claims 1-17 of the '730 patent are unpatentable under 35 U.S.C. § 103 in light of the prior art references and combinations of references presented below. The following rejections should be adopted in their entirety:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1-2, 4-9, 11-12, and 14-17 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 3, 10, and 13 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A. SNQ No. 1: Ludtke in combination with Okereke Renders Claims 1-2, 4-9, 11-12, and 14-17 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1-2, 4-9, 11-12, and 14-17 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

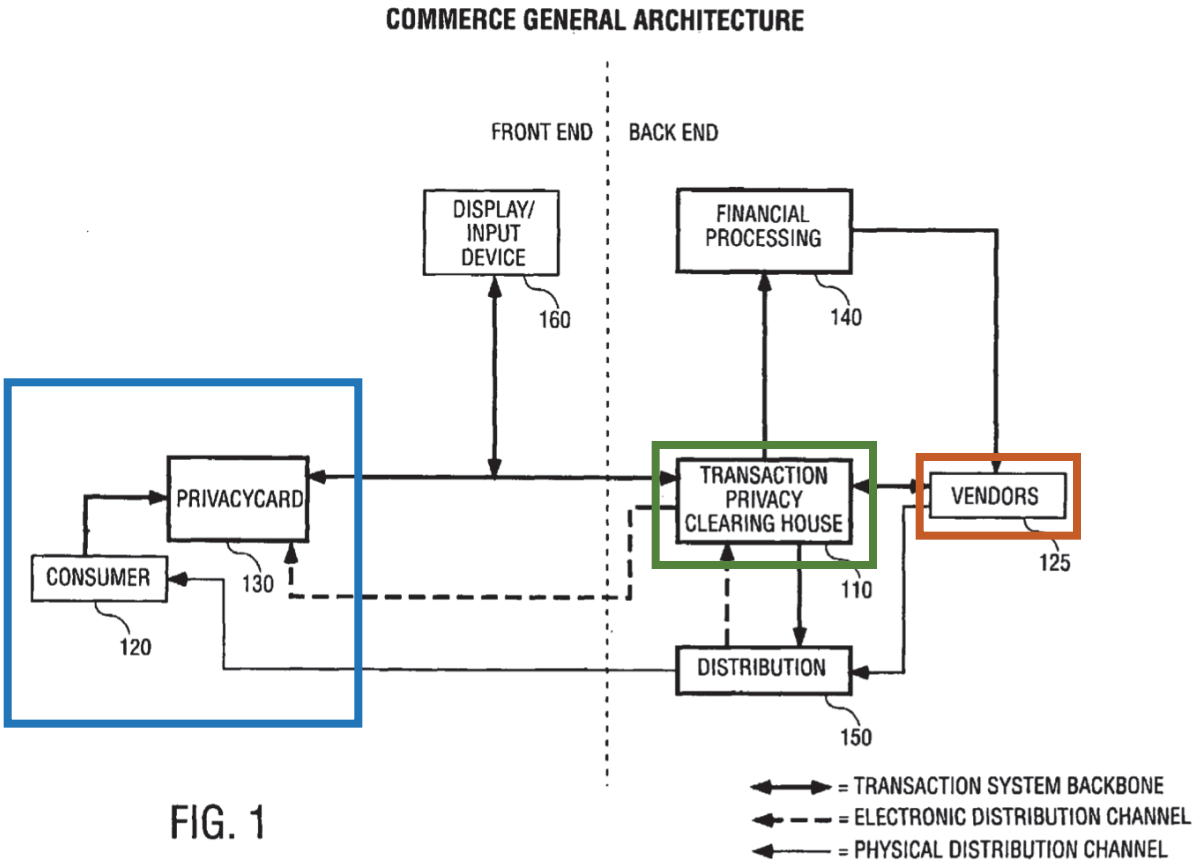


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card , and digital wallet . *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction

between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret information." Specifically, Okereke discloses a "secret key" that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user. Ex. 1006 at ¶25.

The claims also require an "ID code" that is unique and identifies the user's device ("a unique code identifying a device") that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for

authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Okereke, however, does disclose this unique device ID code information, in the form of a unique serial number or SIM number that identifies the user device. *Id*.

(b) POSITA Would be Motivated to Combine Ludtke and Okereke

The scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

Ludtke discloses a persistent, tamper-proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. Ex. 1003 at ¶54. A POSITA would have already known, as of the priority date of the '730 patent, that encryption using a secret key such as that as part of PKI would have been obvious when communicating confidential information. *Id*. A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id*. The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '730 patent, and was a well-established, well-

known method for implementing encryption. *Id*. PKI encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* A POSITA would recognize that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* A POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. *Id.* Okereke simply demonstrates this knowledge prior to the '730 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or a SIM. Ex. 1003 at ¶55. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. Indeed, both references are in

the same field of endeavor as the '730 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:15-18 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("In order to begin using the system via wireless device, the user may be required to provide additional forms of authentication to the CPS, such as password or biometric signature.").

A POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the

transaction device information. A POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed. Ex. 1003 at ¶57.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features. Ex. 1003 at ¶58.

2. Claim 1

(a) [1a] "A method for verifying a user during authentication of an integrated device, comprising the steps of:"

Ludtke discloses a method for verifying a user during authentication of an integrated device. Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device." Ex. 1005 at 3:32-35.

Ludtke's transaction device provides a number of different "integrated" functions, including maintaining bills and bill paying on the device (*id.* at 4:3-6), online shopping (*id*. at 4:7-35), and downloading and accessing electronic catalogs (*id*. at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id*. at 3:49-51), a screen (*id*. at 3:55-57), and a bar code reader (*id*. at 3:61-63).

Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***…" *Id*. at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such as a biometric solution. *Id.* at 4:65-5:1.

Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id*. at 6:36-44. A POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. Ex. 1003 at ¶62. But this knowledge of POSITA is

further embedded within Okereke. *See Id*., *see also* Ex. 1006 at ¶30. As explained above in detail, a POSITA would have been motivated to combine the disclose of Ludtke with the disclosure in Okereke.

Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication". *Id*. at ¶25.

Okereke specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* at ¶25. When authentication is requested, "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id*. "The unique identifier can be a serial number or SIM number, for example." *Id*. A POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. Ex. 1003 at ¶64. Once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication. *Id*.

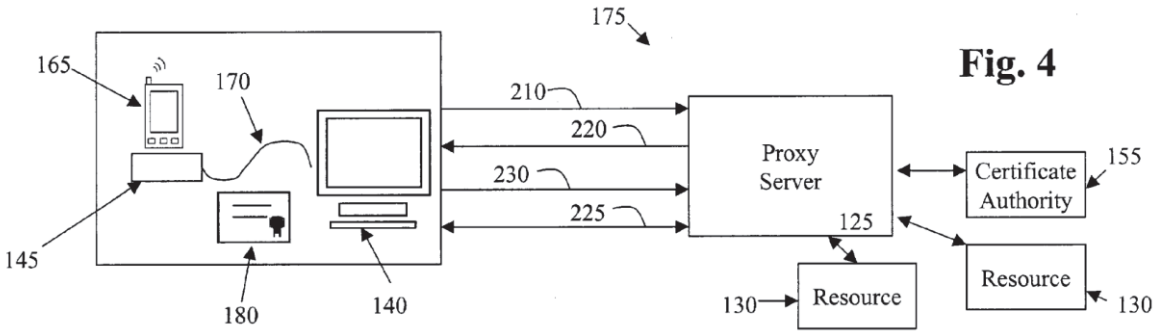


Fig. 4

(b) [1b] persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered wherein the biometric data is selected from a group consisting of a palm print a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition;

Persistently storing biometric data of the user . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered: Ludtke discloses a tamper-proof format on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device in a tamper-proof format that cannot be subsequently altered:

> The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If

> confirmation succeeds, the device writes the fingerprint image data into write once memory, or other memory that is protected from accidental modification.

Ex. 1005 at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). Indeed, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. Ex. 1003 at ¶65. Memory that is protected from accidental modification is also tamper-proof, since it will prevent unauthorized modification—whether by accident, or by someone who might have malicious intent. *Id*. In each case, this tamper-proof memory is persistent storage, because the information stored is not easily re-writable. *Id.*.

Persistently storing . . . a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered: As explained above, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value. Specifically, Okereke discloses in the form of a serial number or SIM number. Ex. 1006 at ¶25. Both serial numbers and SIM numbers are unique codes that identify the devices they are attached to. Ex. 1003 at ¶66. Okereke also discloses a "secret

decryption value." Specifically, Okereke describes a private/public key process. Okereke, for example, describes a Diffie Hellman Key Exchange, which uses AES (Advanced Encryption Standard). "AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications." Ex. 1006 at ¶25. Specifically, the system uses a secret "private key" which can be used to encrypt and decrypt data that is exchanged between the wireless device and other system devices. *Id*. at ¶24, Ex. 1003 at ¶66. The secret key and the ID code together comprise a "plurality of code and other data values."

As discussed above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Okereke and the unique serial numbers and SIMs. Ex. 1003 at ¶67; *see supra* §X.A.1. Specifically, the Okereke device did not include a tamper-proof format that could not be altered, but Ludtke does include such an area of the integrated device. *Id.*. A POSITA would have been motivated to store permanent information, such as the secret key (private key) and unique device identifiers (serial number and/or SIM). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Okereke, which would ensure that the information used to authenticate the device only identifies the authorized device. *Id.*. A POSITA would have stored the unique device

identifiers and the secret key in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information. *Id.*.

Wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition: Ludtke describes a number of different types of biometric information that may be used: "The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, ***retinal scan***, ***voice***, DNA, ***hand profile, face recognition***, etc." Ex. 1005 at 35:60-64.

(c) [1c] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan

Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As explained above, Ludtke describes using biometric verification – including a fingerprint[4] – to verify

[4] Samsung contends that a fingerprint is not within the scope of claim 1. However, Ludtke still discloses the elements of claim 1 in that it discloses different types of biometric information, including those covered by claim 1. *See* Ex. 1005 at 4:66-5:1.

the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input:

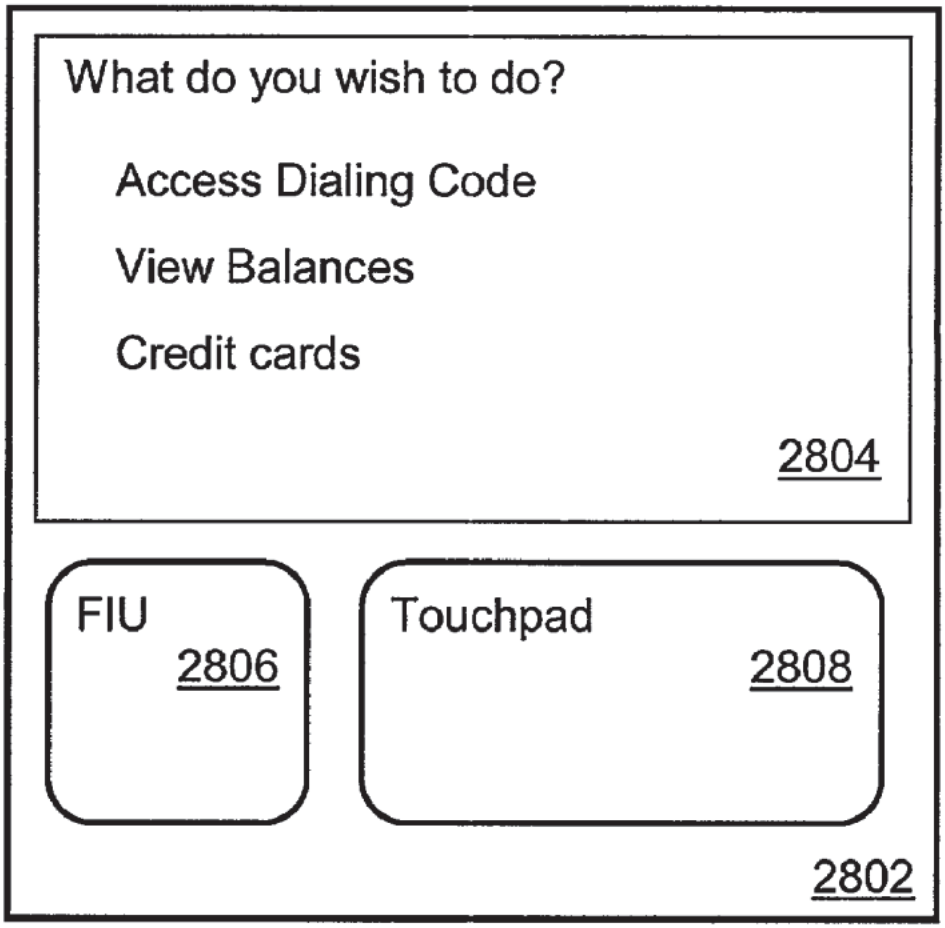


FIG. 28

Ex. 1005 at Fig. 28. "The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." *Id*. at 39:24-27.

Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

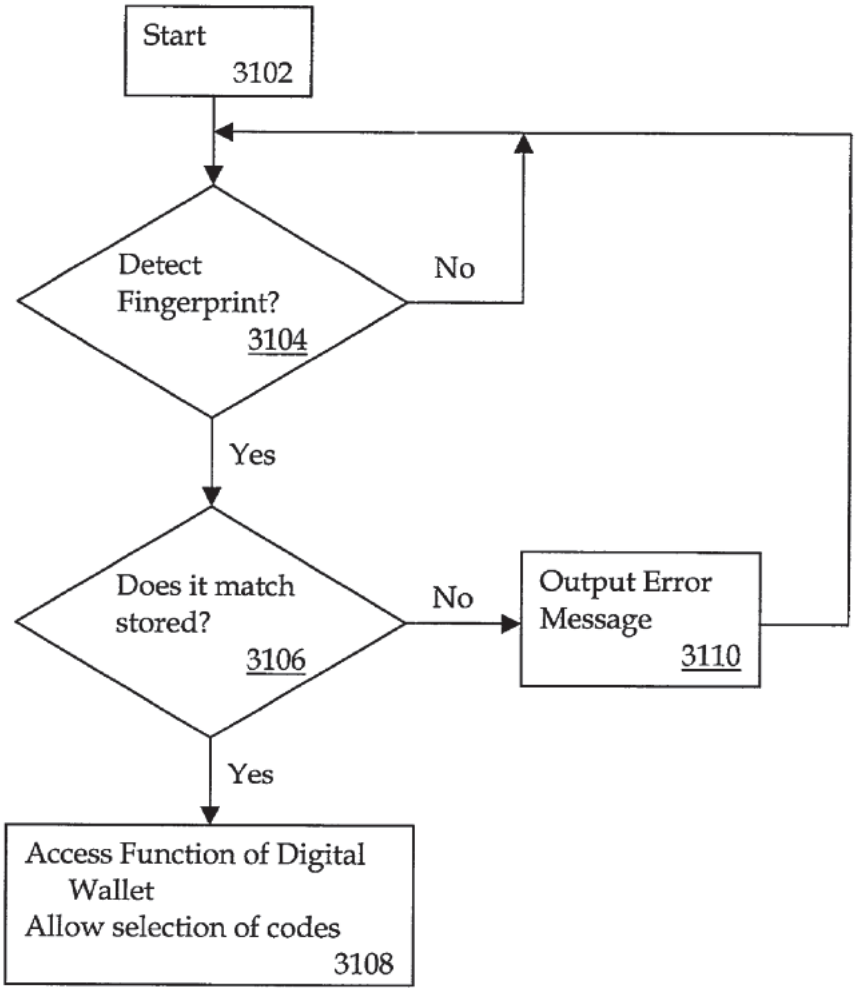


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, the device is continuously looking for a request for verification ("Detect fingerprint"). In response to that request, it

will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). *Id*. at 39:47-59.

(d) [1d] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data

Ludtke also shows this limitation in Figure 31:

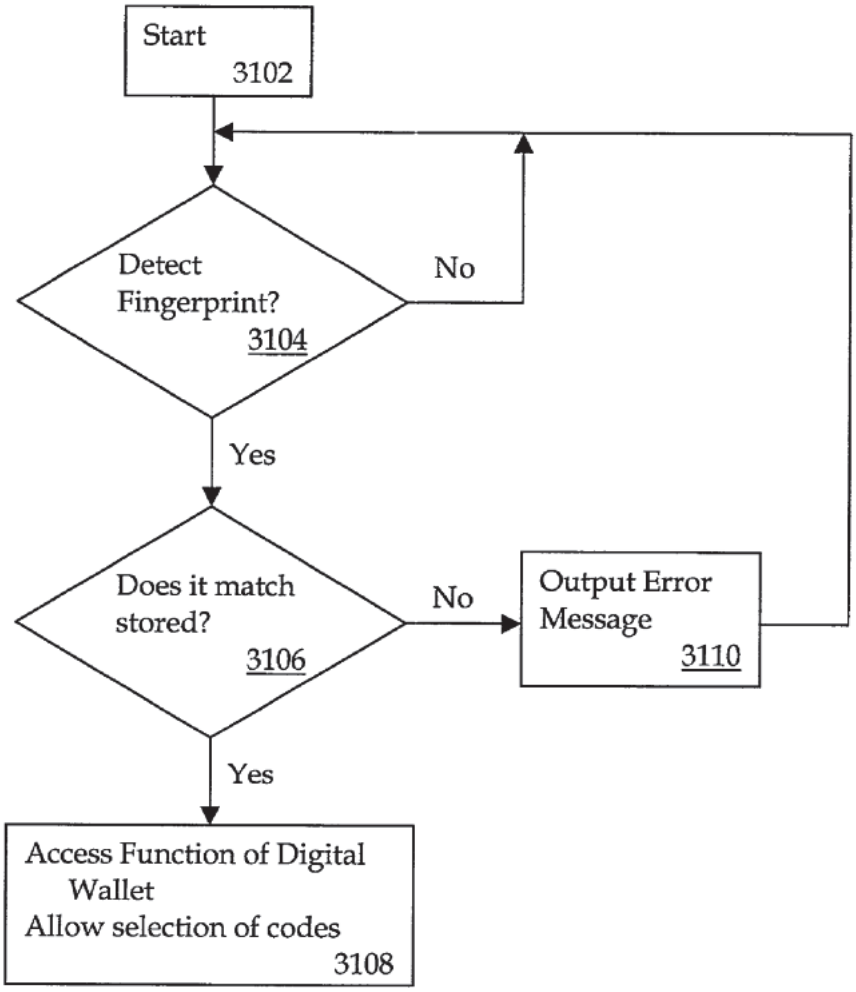


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that if "a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW [Digital Wallet/Integrated Device] returns to checking to see if a fingerprint has been

detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." *Id*. at 39:53-59.

(e) [1e] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

Although this limitation includes citations to "one or more codes from the plurality of codes and the other data values," this is reference to the antecedent basis of this term in [1b] describing the storage of that category of information. The "wherein" clause in this limitation shows that only the device ID code is wirelessly sent. Therefore, of the information required to be stored in the persistent memory, only the Device ID code needs to be sent (although additional information is not precluded from being sent). Taking this into consideration, this limitation can be more easily interpreted as: "responsive to a determination that the scan data matches the biometric data, wirelessly sending [the device ID code] for authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices."

Responsive to a determination that the scan data matches the biometric data: As explained in conjunction with limitation [1d], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id*. at 39:47-54.

Third party trusted authority: Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id*. at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party (i.e., an entity or party separate from the principal parties to the transaction):

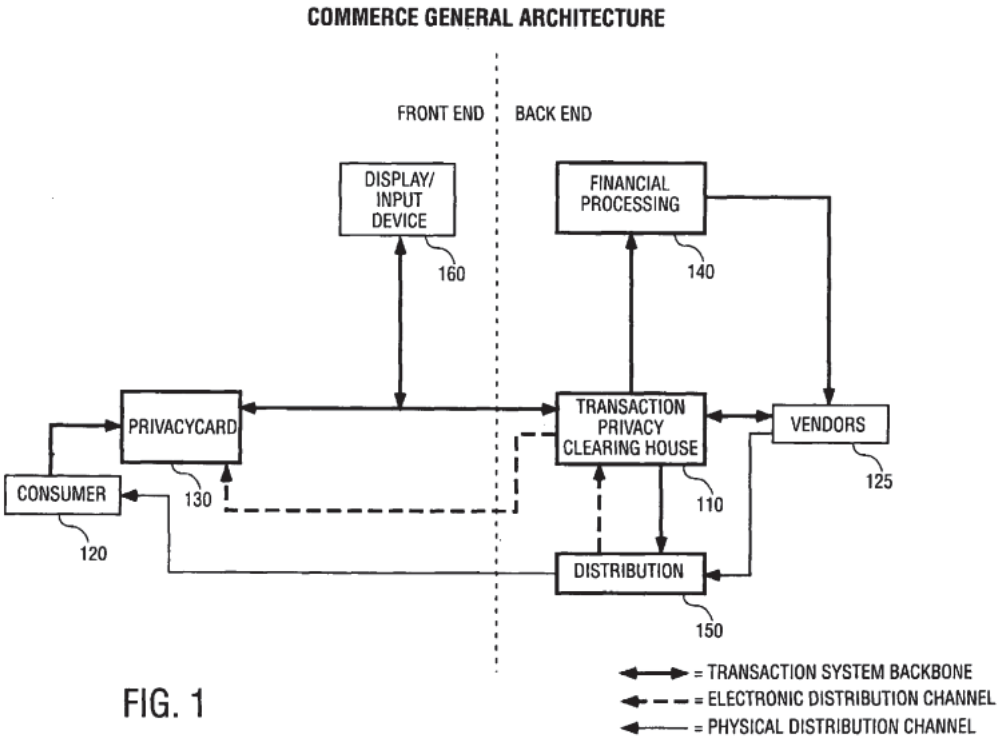


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id*. at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id*. at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id*. "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id*. at 6:36-39.

The TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel.

This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id*. at 7:42-48. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

The TPCH is also a "trusted authority." Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id*. at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete.

The third party trusted authority possesses a list of codes: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction." *Id*. at 6:49-55. And as explained above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id*. at 6:41-44.

Therefore, the TPCH includes information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of Device ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27; Ex. 1003 at ¶78.

Wirelessly sending a code to the third party trusted authority for authorization: Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." Ex. 1005 at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id*. at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id*. at 9:35-42.

Device ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. *Id*. at 6:41-44. However, as discussed above, a

POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a device serial number or SIM code, both of which uniquely identify the integrated device. Ex. 1006 at ¶25; Ex. 1003 at ¶80.

(f) [1f] responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing user access to an application, where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Ludtke teaches this limitation. As explained above, the terms "the one or more code and other data values" can be synthesized into the "Device ID code."

Responsive to authentication of the device ID code by the agent, receiving an access message from the agent allowing user access to an application: In this case, the "agent" is the third party trusted authority. As indicated above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 ***and the user 120*** approval of the transaction to be performed." Ex. 1005 at 6:41-44. A POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. Ex. 1003 at ¶82. In this case, the TPCH sends a signal (or a notification) to the transaction device, which

will allow (enable or announce) access to the application on the transaction device that will permit the transaction to be completed. Ludtke further discloses this limitation at Fig. 15, Step 1520:

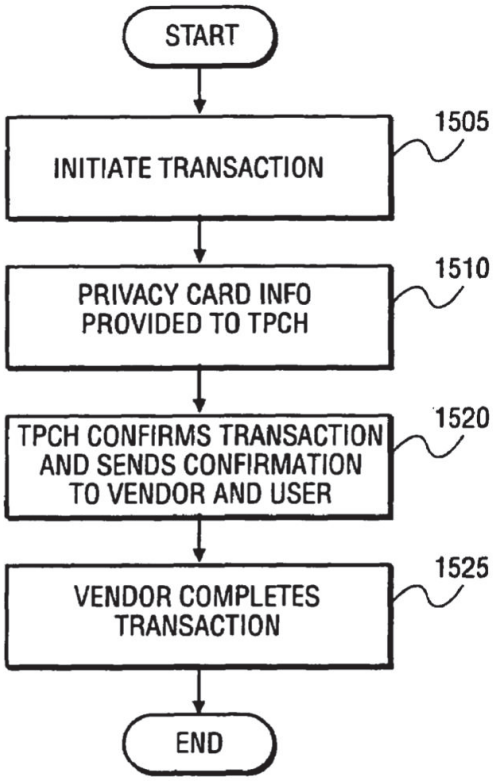


FIG. 15

Ex. 1005 at Fig. 15, *see also* Fig. 17, steps 8-11. With regard to step 1520, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the

confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id*. at 27:13-16.

Where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file: In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which a POSITA would recognize as computer software and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. *See e.g.* Ex. 1005 at Fig. 5a-b, 9:7-25; *see also* Ex. 1003 at ¶83.

3. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network."

As explained above, Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." Ex. 1005 at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id*. at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem

connections, wireless or cellular signals, etc." *Id*. at 9:35-42. Therefore, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network.

4. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."

As explained above, Ludtke includes disclosure where the biometric information is checked to verify the user before they can access the financial application. Ludtke describes this in Figure 31:

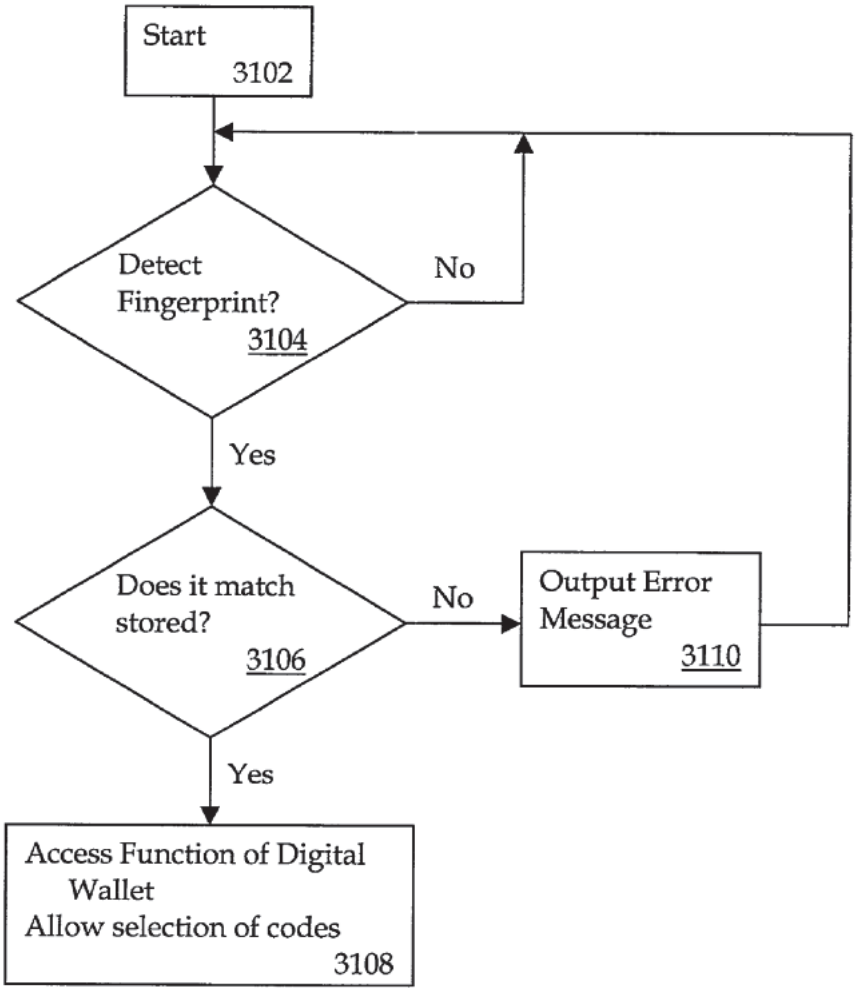


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that if "a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW [Digital Wallet/Integrated Device] returns to checking to see if a fingerprint has been

detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." *Id*. at 39:52-59.

Claim 4 requires only that the verification is part of the "one or more codes or other data values." In claim 1, these codes are stored in the persistent tamper-proof memory. One of ordinary skill in the art would find it obvious to store the verification as part of the codes and other data values in this memory as it relates to the biometric information which is important information that one would not want to be tampered with. Ex. 1003 at ¶87. Moreover, the storage as part of the "one or more codes or other data values" ensures that the verification information is available to be used for other purposes by the device. *Id*.

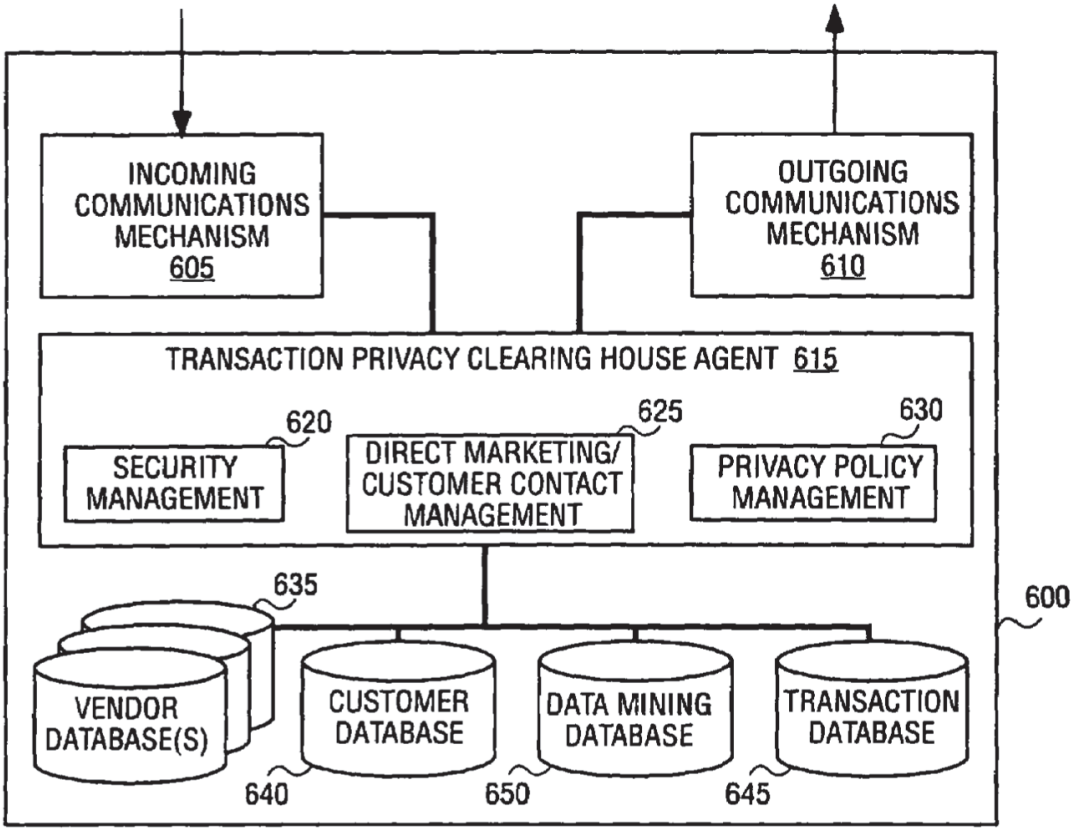
5. Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user."

Ludtke discloses this limitation. Ludtke describes a number of different types of biometric information that may be used, including a fingerprint: "The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, ***fingerprint***, retinal scan, voice, DNA, hand profile, face recognition, etc." Ex. 1005 at 35:60-64..

6. Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to sending

the one or more codes and other data values for authentication"

Ludtke discloses this limitation. This limitation refers to the transaction device establishing a connection for communicating with the TPCH, or third party trusted authority. Ex. 1003 at ¶89. The TPCH includes a security management function 620 responsible for secure communications:



TRANSACTION PRIVACY CLEARING HOUSE: MAJOR COMPONENTS

FIG. 6

Ex. 1005 at Fig. 6. "The security management function 620 ensures secure communications among the components internal to the TPCH 600 and the external entities external to the TPCH 600. This ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account." *Id*. at 9:52-59. Therefore, with the security management 620, the transaction devices communicate with the TPCH 600 via a secure communication channel.

7. Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."

Ludtke discloses this limitation. Ludtke envisions using different forms of authentication other than biometric information. Ludtke states: "One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (*e.g.*, fingerprint recognition)." Ex. 1005 at 4:65-5:1. In the situation where a PIN was used, there would be no need for a request for biometric information. Ex. 1003 at ¶90.

8. Claim 8:

(a) [8a] "An integrated device for verifying a user during authentication of the integrated device, comprising."

Ludtke and Okereke disclose an integrated device for verifying a user during authentication of the integrated device. *See* Element [1a], Section X.A.2.a, *supra*.

(b) [8b] "a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;"

Ludtke and Okereke disclose this element. *See* Element [1b], Section X.A.2.b, *supra*.

(c) [8c] "a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

Ludtke discloses this limitation. *See* Elements [1c-1e], Sections X.A.2.c-e, *supra*.

The "verification unit" will be the portion of memory and instructions that verify the biometric information. Ex. 1003 at ¶94. A POSITA would recognize that the verification unit would be in communication with the memory, since the biometric information that the verification unit compares with received biometric information is stored in the memory for comparison. *Id*.

(d) [8d] responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Ludtke discloses this limitation. *See* Element [1f], Section X.A.2.f, *supra*.

9. Claim 9: "The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network."

See Claim 2. Section X.A.3, *supra*.

10. Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."

Ludtke discloses notifications to request a biometric scan and it would be obvious to use an LED. In describing the fingerprint scanner, Ludtke indicates that at "various times during interaction, the user is prompted to supply a fingerprint recognition sample." Ex. 1005 at 14:40-42. A POSITA would recognize that the

prompt can be in a number of ways that would be consistent with alerts on a mobile device. Ex. 1003 at ¶97. One of the common alert mechanisms in a mobile device is an LED. *Id*. Ludtke further discloses a user interface:. For example, figure 28 shows a device with a screen 2804 that asks a user what they wish to do:

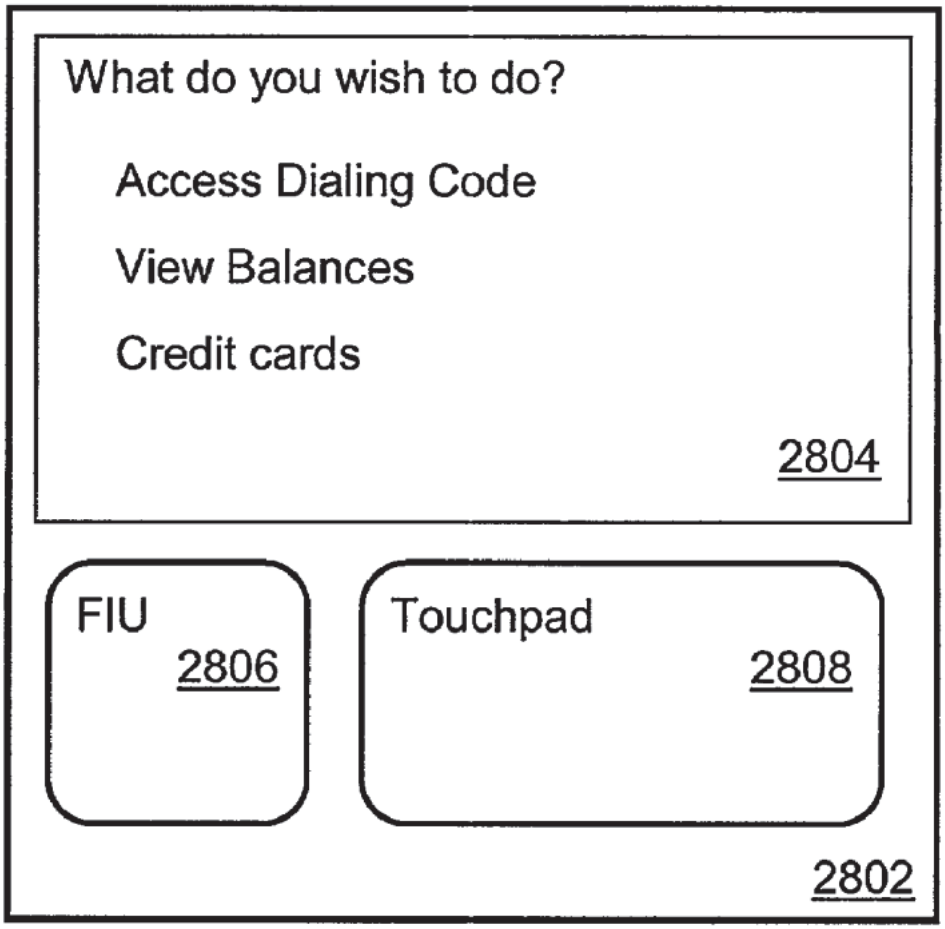


FIG. 28

Ex. 1005 at Fig. 28. POSITA would have recognized that user interface screens such as these are very often implemented with an LED screen, and an LED screen would be the obvious choice for alerting the user.

11. Claim 12

(a) [12a]. "A method for authenticating a verified user using a computer processor configured to execute method steps, including:"

Ludtke and Okereke disclose this limitation. *See* Element [1a]. Section X.A.2.a, *supra*.

It is inherent that any steps needed to authenticate the verified user would be executed using a computer processor. Ex. 1003 at ¶99.

(b) [12b]. "receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices"

Ludtke and Okereke disclose this limitation. See Elements [1b], [1e], Sections X.A.2.b, X.A.2.e, *supra*. The claim does not specifically indicate what "receives" the one or more codes, and therefore, the receiver can be the device itself, a memory or processor on the device, or another device receiving the codes. Ex. 1003 at ¶101.

Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. This means Ludtke discloses "biometrically verified users."

A POSITA would recognize that in order for the transaction device's information to be present in the TPCH, the information would need to be registered with the TPCH. *Id.* at ¶102. The registration process ensures that the information is stored on the TPCH when it authenticates the device. *Id.*

(c) [12c] "requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;"

Ludtke discloses this limitation. *See* element [1e], section X.A.2.e, *supra*. Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." Ex. 1005 at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id*. at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id*. at 9:35-42. A POSITA would recognize that when the transaction device information is sent to the agent, it is a request for authentication.

Ex. 1003 at ¶103. When the TPCH approves the transaction, it is indicating that the codes and other data [transaction device information] is legitimate. *Id*.

(d) [12d] receiving an access message from the agent; and

Ludtke discloses this limitation. *See* element [1f], section X.A.2.f, *supra*.

(e) [12e] in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine , a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a website and a file.

Ludtke discloses this limitation. *See* element [1f], section X.A.2.f, *supra*.

12. Claim 14: "The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or mode codes and the other data values associated with the biometrically verified user is received from the biometric key."

Ludtke discloses this limitation. *See* Claim 6, section X.A.6, *supra*. This claim indicates that the "one or more codes and the other data values associated with the biometrically verified user" are stored on a "biometric key" before being transferred to the third party trusted authority. The memory where these values are stored on the Ludtke user device is a "biometric key" because it is accessed when the user is verified with biometric information, giving access to the data on the device, and eventually allowing authentication by the TPCH. Ex. 1005 at 4:62-5:1; Ex. 1003 at ¶106.

13. Claim 15

(a) [15a] a system, comprising:

Ludtke discloses this limitation. Specifically, Ludtke discloses a system for transactions between a transaction device 130 being used by a consumer 120, and a vendor 125, with authorization performed by the transaction privacy clearing house 110, as shown in Figure 1:

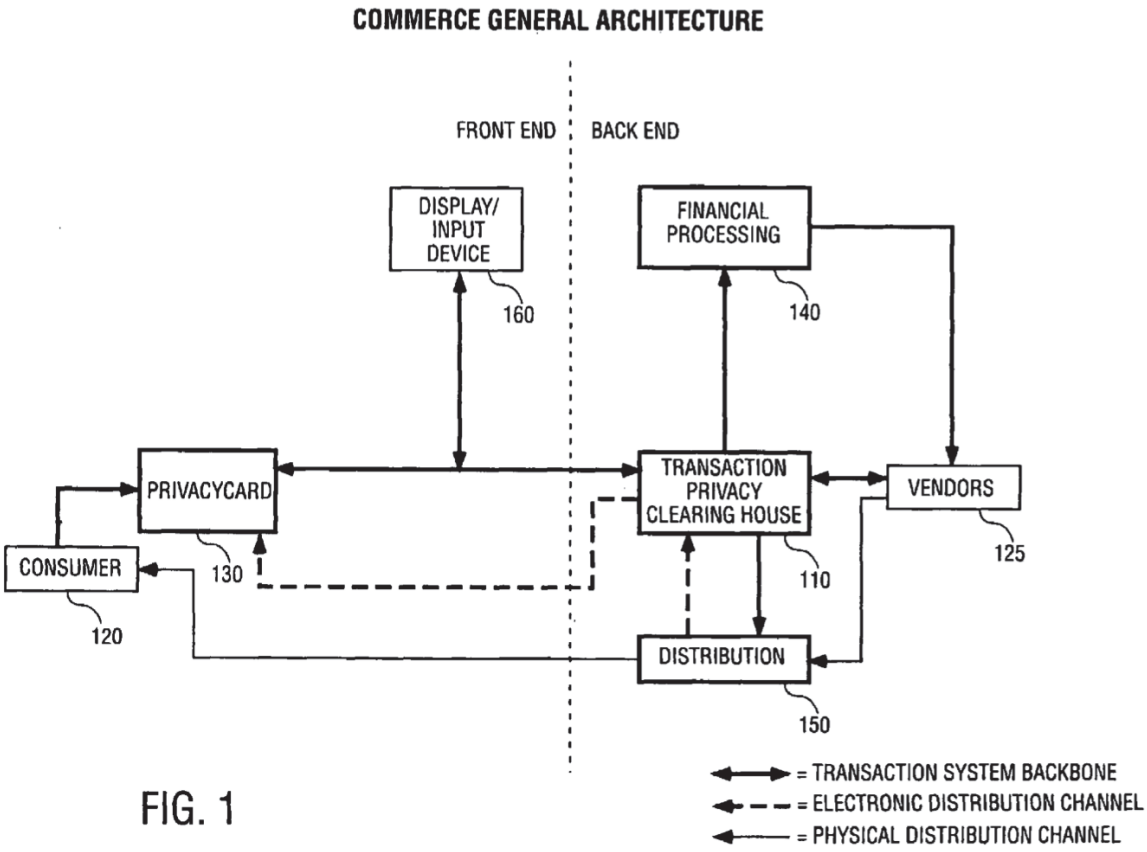


FIG. 1

(b) [15b] a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a

tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,

Ludtke and Okereke disclose this limitation. *See* element [1b], section X.A.2.b, *supra*. This claim uses the term "biometric key" to refer to the device the user uses (known in other claims as an "integrated device.")

(c) [15c]: "and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition; and"

Ludtke and Okereke disclose this limitation. *See* claim elements [1b], [1d], and [1e], sections X.A.2.b, d, e, *supra*.

(d) [15d]: "an authentication unit receives the plurality of codes and the other data values and send[] the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third party trusted authority possessing a list of device ID codes uniquely identifying integrated devices,"

Ludtke and Okereke disclose this limitation. *See* claim element [1e], section X.A.2.e, *supra*. Here, the "authentication unit" is code on a processor on

the integrated device that is responsible for sending the Device ID code or additional codes to the third party trusted authority to authenticate the user and device. Ex. 1003 at ¶110.

(e) [15e]: "and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, and a file."

Ludtke discloses this limitation. *See* claim element [1f], section X.A.2.f, *supra*.

14. Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data."

Ludtke discloses this limitation. *See* claim element [1c], section X.A.2.c, *supra*.

15. Claim 17: "The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values."

Ludtke discloses this limitation. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

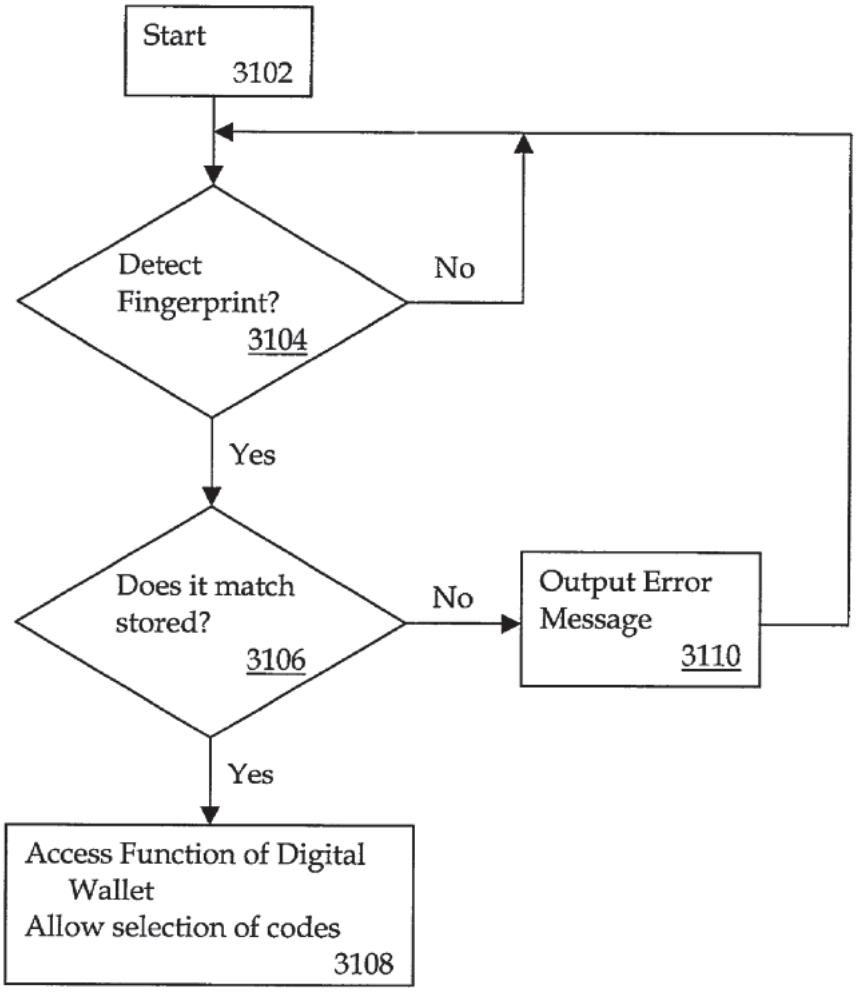


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, if the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes. *Id*. at 39:47-59.

B. SNQ No. 2: Ludtke in combination with Okereke and Robinson Renders Claims 3, 10, and 13 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as outlined in SNQ 1, but also relies on Robinson for the limitations in dependent claims 3, 10, and 13. All three of these dependent claims involve registering an age verification. Where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 3, 10, and 13. As explained below, POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke.

(b) POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Okereke. Ex. 1003 at ¶116. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1..

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or

transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10; Ex. 1003 at ¶117. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. Ex. 1003 at ¶117.

POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Ex. 1003 at ¶118. Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. Ex. 1003 at ¶118. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id*.

2. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section X.A.2, *supra*.

However, neither Ludtke nor Okereke expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson (US2003/0177102) discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67 Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user.

3. Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.

Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section X.A.9, *supra*.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 10 for the same reasons as described in conjunction with claim 3. Section X.B.2, *supra*.

4. Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent."

Ludtke in combination with Okereke disclose all of the limitations of claim 12. *See* SNQ 1, Claim 12. Section X.A.11, *supra*.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 13 for the same reasons as described in conjunction with claim 3. Section X.B.2, *supra*.

C. SNQ No. 3: Ludtke in combination with Scott Renders Claims 1-2, 4-9, 11-12, and 14-17 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1-2, 4-9, 11-12, and 14-17 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

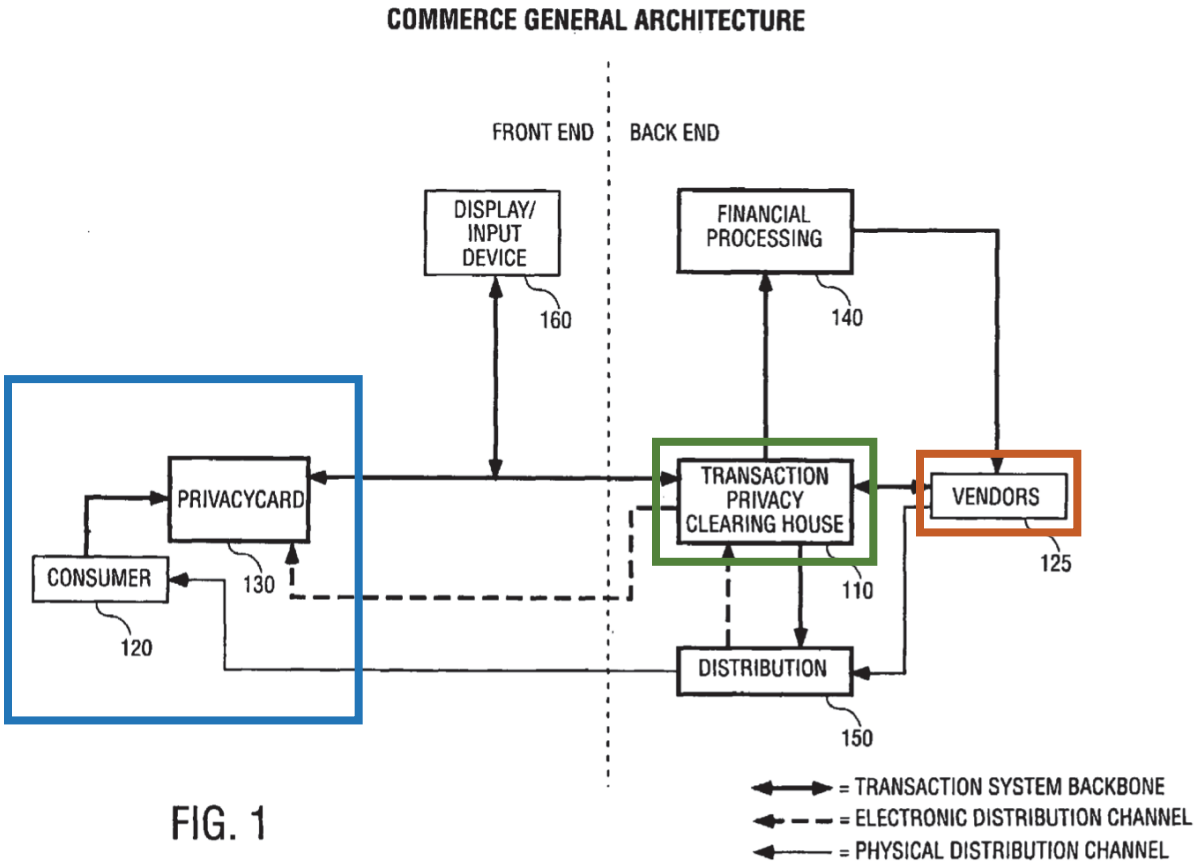


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction

between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id*. at 8:21-22.

Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this

"transaction device information" is unique and identifies the consumer's transaction device. Scott, however, does disclose an ID code that is unique and identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(b) POSITA Would be Motivated to Combine Ludtke and Scott

The scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16

Ludtke discloses a persistent, tamper proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. Ex. 1003 at ¶130. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. *Id.* As discussed above, a POSITA would have already known, as of the priority date of the '730 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. *Id.* A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '730 patent, and was a well-established, well-known method for implementing encryption. *Id.*. For example, Public Key Cryptography, later developed into PKI encryption well before the '730 patent, was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* A POSITA would therefore recognize that the use of secret information, which is disclosed in Scott,

would make the system of Ludtke even more secure. *Id.* Scott simply demonstrates this knowledge prior to the '730 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Ex. 1003 at ¶131. Scott explicitly discloses this fundamental information. *Id*.

A POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '730 patent, *i.e.*, authentication of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:15-18 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("A method of identifying an authorized user with a biometric

device and enabling the authorized user to access private information over a voice network is disclosed"); Ex. 1008 at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…").

A POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed. Ex. 1003 at ¶133.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Scott. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features. Ex. 1003 at ¶134.

2. Claim 1

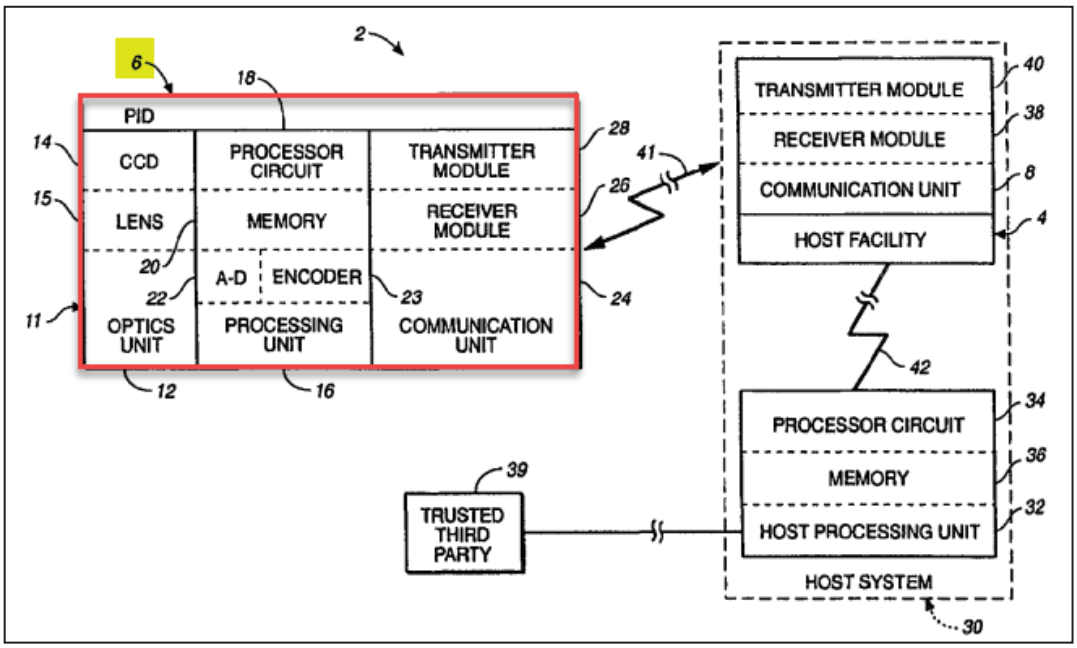
(a) [1a] "A method for verifying a user during authentication of an integrated device, comprising the steps of:"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.a, *supra*.

As explained above in detail, a POSITA would have been motivated to combine the disclose of Ludtke with the disclosure in Scott.

Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a

point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

(b) [1b] persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered wherein the biometric data is selected from a group consisting of a palm print a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition;

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.b, *supra*.

Persistently storing . . . a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered: As explained above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. A serial number is a unique code that identifies the device it is attached to. Ex. 1003 at ¶139. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." Ex. 1008 at 6:28-7:23, 13:10-15, 19:30-32

Scott also discloses a "secret decryption value." Specifically, Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." *Id.* at 11:24-30, 28:13-15, 4:14-18. Scott also discloses that the private key used by the PID 6 is never disclosed. *Id.* at 8:21-22. The PID 6 uses its private key to encrypt a

transmission to a host system. *Id.* at 17:9-12. The host system uses a corresponding public key to decrypt the transmission. *Id.* Thus, a POSITA would have recognized the benefits of increased security and privacy by using the private/public key pair to protect all transmissions between PID 6 and host facility 4. Ex. 1003 ¶140. Scott's PID 6 would thus use its private key to decrypt messages such as, for example, a random number signal for verification (Ex. 1008 at 17:32-18:2, 27:4-17), that were encrypted with the corresponding public key at the host system. Ex. 1003 ¶140.

As discussed above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Scott and the unique serial numbers also disclosed in Scott. *Id.* ¶141; *see supra* §X.C.1. A POSITA would have been motivated to store permanent information, such as the secret key (private key) and unique device identifiers (serial number). Moreover, POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. Ex. 1003 at ¶141. A POSITA would also have stored the unique device identifiers and the secret key in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications

to take place, and a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information. *Id.* ¶141.

(c) [1c] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.c, *supra*.

(d) [1d] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.d, *supra*.

(e) [1e] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.e, *supra*.

Device ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. Ex. 1005 at 6:36-64. However, as discussed above,

POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include a device serial code which uniquely identify the integrated device. Ex. 1008 at 4:1-14, 5:10-21; Ex. 1003 at ¶145.

(f) [1f] responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing user access to an application, where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.f, *supra*.

3. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.3, *supra*.

4. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.4, *supra*.

5. Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.5, *supra*.

6. Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to sending the one or more codes and other data values for authentication"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.6, *supra*.

7. Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.7, *supra*.

8. Claim 8:

(a) [8a] "An integrated device for verifying a user during authentication of the integrated device, comprising."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8.a, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1a], Section X.C.2.a, *supra*

(b) [8b] "a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8.b, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1b], Section X.C.2.b, *supra*

(c) [8c] "a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8.c, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Elements [1c-1e], Sections X.C.2.c-e, *supra*

(d) [8d] responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8.d, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section X.C.2.f, *supra.*

9. Claim 9: "The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network."

See Claim 2. Section X.C.3, *supra*.

10. Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8.10, *supra*.

11. Claim 12

(a) [12a]. "A method for authenticating a verified user using a computer processor configured to execute method steps, including:"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11.a, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1a], Section X.C.2.a, *supra*

(b) [12b]. "receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11.b, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Elements [1b], [1e], Section X.C.2.b, X.A.2.e, *supra*

(c) [12c] "requesting authentication of the one or more codes and the other data values by the agent, wherein

the authentication determines whether the one or more codes and the other data values are-legitimate;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11.c, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1e], Section X.C.2.e, *supra*

(d) [12d] receiving an access message from the agent; and

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11.d, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section X.C.2.f, *supra*

(e) [12e] in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine , a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a website and a file.

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11.e, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section X.C.2.f, *supra*

12. Claim 14: "The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or mode codes and the other

data values associated with the biometrically verified user is received from the biometric key."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12, *supra*.

13. Claim 15

(a) [15a] a system, comprising:

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13.a, *supra*.

(b) [15b] a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13.b, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1b], Section X.C.2.b, *supra*.

(c) [15c]: "and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial

recognition, a signature recognition, and a voice recognition; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13.c, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Elements [1b], [1d], and [1e], Section X.C.2.b, d, e, *supra*.

(d) [15d]: "an authentication unit receives the plurality of codes and the other data values and send[] the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third party trusted authority possessing a list of device ID codes uniquely identifying integrated devices,"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13.d, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1e], Section X.C.2.e, *supra*

(e) [15e]: "and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM

machine, a hard drive, computer software, a web site, and a file."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13.e, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section X.C.2.f, *supra*

14. Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.14, *supra*.

Ludtke and Scott disclose this limitation. *See* Claim element [1c], Section X.C.2.c, *supra*

15. Claim 17: "The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.15, *supra*.

D. SNQ No. 4: Ludtke in combination with Scott and Robinson Renders Claims 3, 10, and 13 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined in SNQ 3, but also relies on Robinson for the limitations in dependent claims 3, 10, and 13. All three of these dependent claims involve registering an age verification. Where Ludtke and Scott do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 3, 10, and 13. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Scott.

(b) POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Scott. Ex. 1003 at ¶187. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or

transactions initiated by a wireless device like Ludtke's transaction device. Ex. 1007 at ¶9-10; Ex. 1003 at ¶188. A POSITA would have reocgnized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. Ex. 1003 at ¶188.

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Ex. 1003 at ¶189. Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. Ex. 1003 at ¶189. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id*.

2. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section X.C.2, *supra*.

However, neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section X.B.2.

3. Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 9. Section X.C.9, *supra*.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 10 for the same reasons as described in conjunction with claim 3. Section X.D.2, *supra*.

4. Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent."

Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 12. Section X.C.11, *supra*.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 13 for the same reasons as described in conjunction with claim 3. Section X.D.2, *supra*.

XI. REAL PARTIES OF INTEREST

Requestor certifies that Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. are the real parties-in-interest.

XII. CONCLUSION

For at least the reasons cited herein, the prior art references cited in this Request present substantial new questions of patentability with respect to the Challenged Claims of the ’730 patent. Accordingly, the Office should declare a reexamination of these claims and reject them on at least the SNQs detailed in this Request.

DATED: June 8, 2022

Respectfully submitted,

By */s/ Marissa Ducca*

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.